REMARKS

Claims 1-9, 12-17, 19-21, 23-41, and 45-47 are currently pending in the subject application and are presently under consideration. Claims 1, 12, 16-17, 24, 26, 30, 39, and 41 have been amended as shown on pages 2 to 9 of the Reply. Applicants' representative appreciates courtesies extended by the Examiner in the telephonic interview for the subject application conducted on October 21, 2008, where no agreement was reached as to the subject claims. Favorable reconsideration of the subject patent application is respectfully requested in view of the comments and amendments herein.

I. Rejection of Claims 1-9, 12-17, 19-21, 23-41, and 45-47 Under 35 U.S.C. §102(b)

Claims 1-9, 12-17, 19-21, 23-41, and 45-47 stand rejected under 35 U.S.C. §102(b) as being anticipated by Swiler, *et al.* (US 7,013,395). It is respectfully requested that this rejection be withdrawn for at least the following reasons. Swiler, *et al.* fails to disclose or suggest each and every element recited in the subject claims.

> A single prior art reference anticipates a patent claim only if it expressly or inherently describes ***each and every limitation set forth in the patent claim***. *Trintec Industries, Inc. v. Top-U.S.A. Corp.,* 295 F.3d 1292, 63 USPQ2d 1597 (Fed. Cir. 2002); *See Verdegaal Bros. v. Union Oil Co. of California,* 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987).

The subject matter as claimed generally relates to generating a set of security guidelines, security data, and/or security components for industrial controllers in an industrial automation environment. In particular, input can be received in the form of an abstract description or model of a factory, where the factory description can include information regarding the industrial controllers. The generated security data can include a set of recommended security components, related interconnection topology, connection configurations, application procedures, security policies, rules, user procedures, and/or user practices related to the industrial controllers. Additionally, based on generated data, measures can be taken to improve security in the automation environment. In another example, industrial controllers can be monitored to learn behavior related thereto where deviating from the behavior can cause generation of security data (*e.g.*, data indicating the change, specification of one or more recommended measures,

automated activities based on the recommended measures, *etc.*). To this end, claim 1 as amended recites, in part, ***a validation component that periodically monitors the industrial network controllers following deployment of the one or more security outputs to determine one or more vulnerabilities related thereto***. Swiler, *et al.* fails to disclose such claimed aspects.

Swiler, *et al.* generally relates to a tool that analyzes computer systems for related security attributes. (*See*, Abstract). In particular, Swiler, *et al.* appears to contemplate generating an attack graph based at least in part on inputs including attack templates, configuration files, and attacker profiles. Swiler, *et al.* generally contemplates security analysis for computers, such as "workstations, servers, or routers." (*See e.g.*, column 4, lines 48-52), and creates the attack graph upon request. However, Swiler, *et al.* fails to disclose or suggest ***a validation component that periodically monitors the industrial network controllers following deployment of the one or more security outputs to determine one or more vulnerabilities related thereto***, as recited in claim 1.

On the contrary, Swiler, *et al.* generates the attack graph to show possible insufficiencies in security of a computer network. Swiler, *et al.*, however, is completely silent regarding monitoring or other persistent activities as recited in claim 1. Moreover, Swiler, *et al.* does not teach or suggest deploying security outputs, much less determining vulnerabilities related to industrial controllers following the deployment. Swiler, *et al.* merely generates a graph of possible network intrusions. This is not indicative of deploying security outputs to a network, and periodically monitoring controllers of the network for related vulnerabilities. Moreover, Swiler, *et al.* does not contemplate operability with industrial network controllers. Swiler, *et al.* is concerned merely with computer networks. Industrial controllers, though able to interface with conventional networks, typically have outputs to control industrial assets. Swiler, *et al.* does not disclose or suggest assessing securing considerations of such controllers. For at least these reasons, Swiler, *et al.* fails to disclose or suggest each and every element recited in claim 1.

Moreover, claim 12, as amended, recites in part, *monitoring access to the industrial controllers to* ***learn at least one access pattern*** *and* ***performing one or more automated actions based at least in part on detecting a deviation from the at least one learned access pattern***. Swiler, *et al.* additionally fails to teach these aspects. The Examiner broadly asserts that Swiler, *et al.* teaches learning access patterns by stating that claim 12 is rejected for the same reasons as claim 1 and citing the entire description portion of the reference. Swiler, *et al.*, however, does

not contemplate learning access patterns; though Swiler, *et al.* appears to claim polling computers in a dependent claim, this is not indicative of learning access patterns thereof. In addition, Swiler, *et al.* is completely silent regarding the additional aspects of ***performing one or more automated actions based at least in part on detecting a deviation from the at least one learned access pattern***. Thus, Swiler, *et al.* additionally fails to disclose or suggest all aspects of claim 12. Furthermore, claim 16 recites similar aspects as well, namely *means for* ***detecting a deviation from the at least one access pattern*** *and means for* ***performing an automated action based at least in part on the detected deviation***. Again, Swiler, *et al.* is completely silent in regard to these aspects. Thus, Swiler, *et al.* does not disclose or suggest all aspects of claim 16.

In addition, claim 17 as amended recites additional aspects not contemplated by Swiler, *et al*. In particular, the claim recites, in part, *a security analysis tool that* ***recommends interconnection of one or more industrial automation devices to achieve a specified security goal***. Swiler, *et al.* fails to disclose or suggest such aspects. Not only is Swiler, *et al.* silent regarding recommending interconnection of any devices, it is definitely silent regarding interconnection with industrial automation devices as it does not contemplate such devices. Thus, Swiler, *et al.* does not disclose or suggest all aspects of claim 17. In addition, claim 24 has been amended to recite *a component to* ***automatically install one or more security components in response to detected security problems***. Swiler, *et al.* does not contemplate this functionality either.

Further, claim 26 as amended recites ***performing an automated security procedure on the one or more industrial automation devices based at least in part on the potential security violations*** *and* ***determining whether the industrial automation device conforms to one or more industry standards following performing the automated security procedure thereon***. Swiler, *et al.* is silent regarding both aspects. Swiler, *et al.* does not teach or suggest performing automated security procedures based on potential security violations – only creating threat maps, as described. Thus, Swiler, *et al.* is additionally silent regarding determining whether an industrial automation device conforms to an industry standard based on the procedure performed. For at least these reasons, Swiler, *et al.* also fails to disclose each and every element of claim 26.

Additionally, claim 30 as amended recites, in part, *means for performing at least one of security assessments, security compliance checks, and security vulnerability scanning of the industrial automation devices to mitigate the security violations* ***based at least in part on the***

initiated security procedure. Swiler, *et al.*, as shown, fails to disclose or suggest performing security procedures. To the extent the Examiner interprets generating the map as a security procedure, there is no subsequent performing security assessments, compliance checks, or vulnerability scanning as recited. Thus, Swiler, *et al.* additionally fails to disclose or suggest all elements recited in claim 30.

Also, claim 31 recites *a learning component to* ***monitor and learn industrial automation activities*** *during a training period and a detection component to* ***automatically trigger a security event based upon detected deviations of subsequent industrial automation activities*** *after the training period*. As shown, Swiler, *et al.* fails to disclose or suggest learning industrial automation activities; rather, Swiler, *et al.* merely generates an attack graph for a computer network. Moreover, however, Swiler, *et al.* fails to disclose or suggest detecting deviations from the activities, much less automatically triggering security events based on such. Thus, Swiler, *et al.* fails to disclose or suggest all elements of claim 31 as well.

Furthermore, claim 39 recites similar learning functionalities of claim 31, which Swiler, *et al.* does not teach or suggest; the claim also recites ***generating an alarm where a current data pattern is determined to be outside of a predetermined threshold associated with the at least one data pattern***. Swiler, *et al.* neither discloses nor suggests determining current data patters to be outside of predetermined patterns or generating an alarm or performing any activity based on such a determination. Claim 41 recites similar aspects, namely *means for* ***generating a security event where the access patterns are determined to be out of tolerance from stored access patterns***. Swiler, *et al.* fails to disclose these aspects as shown. Thus, Swiler, *et al.* fails to disclose each and every element recited in claims 39 and 41.

In view of at least the foregoing, it is readily apparent that Swiler, *et al.* fails to disclose or suggest each and every element recited in claims 1, 12, 16, 17, 26, 30, 31, 39, and 41. Accordingly, it is respectfully requested that rejection of these claims, as well as claims 2-9, 13-15, 19-21, 23-25, 27-29, 32-38, 40, and 45-47, which depend therefrom, be withdrawn.

CONCLUSION

The present application is believed to be in condition for allowance in view of the above comments and amendments. A prompt action to such end is earnestly solicited.

In the event any fees are due in connection with this document, the Commissioner is authorized to charge those fees to Deposit Account No. 50-1063 [ALBRP303USC].

Should the Examiner believe a telephone interview would be helpful to expedite favorable prosecution, the Examiner is invited to contact applicants' undersigned representative at the telephone number below.

Respectfully submitted,

AMIN, TUROCY & CALVIN, LLP

/David Matthew Noonan/
David Matthew Noonan
Reg. No. 59,451

AMIN, TUROCY & CALVIN, LLP
57TH Floor, Key Tower
127 Public Square
Cleveland, Ohio 44114
Telephone (216) 696-8730
Facsimile (216) 696-8731